Recon-ng: Compréhensive Reconnaissance Guide

Introduction

What is Recon-ng?

Recon-ng is a full-featured reconnaissance framework written in Python. It provides a powerful environment for conducting open-source web-based reconnaissance quickly and thoroughly.

What is Recon-web?

Recon-web is the web interface for Recon-ng, providing a user-friendly GUI to interact with the Recon-ng framework through a browser.

Why Use These Tools?

- **Automated OSINT**: Gather intelligence from public sources automatically
- **Modular Design**: Use only the modules you need
- **Data Management**: Organize findings in a structured database
- **Professional Reporting**: Generate comprehensive reports for penetration testing

Prerequisites

System Requirements

- Kali Linux (running on Oracle VirtualBox)
- Python 3.6 or higher
- Internet connection
- At least 2GB RAM allocated to VM
- 20GB free disk space

Required Knowledge

- Basic Linux command line
- Understanding of networking concepts
- Familiarity with OSINT techniques
- Basic cybersecurity principles

Installation

Step 1: Update Kali Linux

bash

sudo apt update && sudo apt upgrade -y

Step 2: Install Recon-ng

bash

sudo apt install recon-ng -y

Step 3: Verify Installation

bash

recon-ng --version

Step 4: Install Recon-web (Optional)

bash

cd /opt

sudo git clone https://github.com/lanmaster53/recon-web.git

cd recon-web

sudo pip3 install -r requirements.txt

Practical Walkthrough

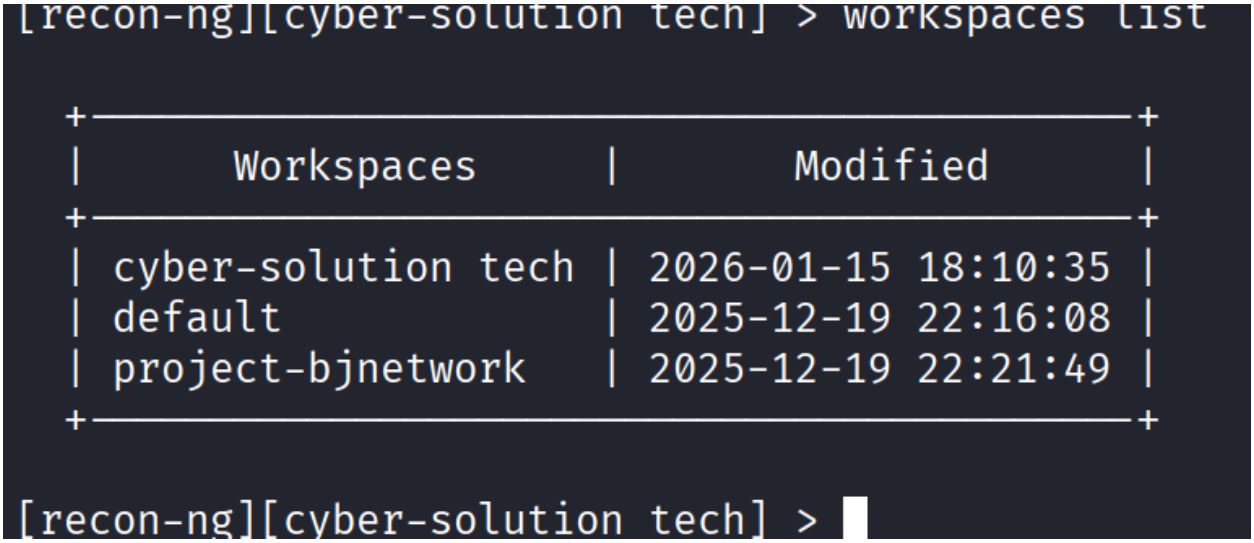
Phase 1: Workspace Setup

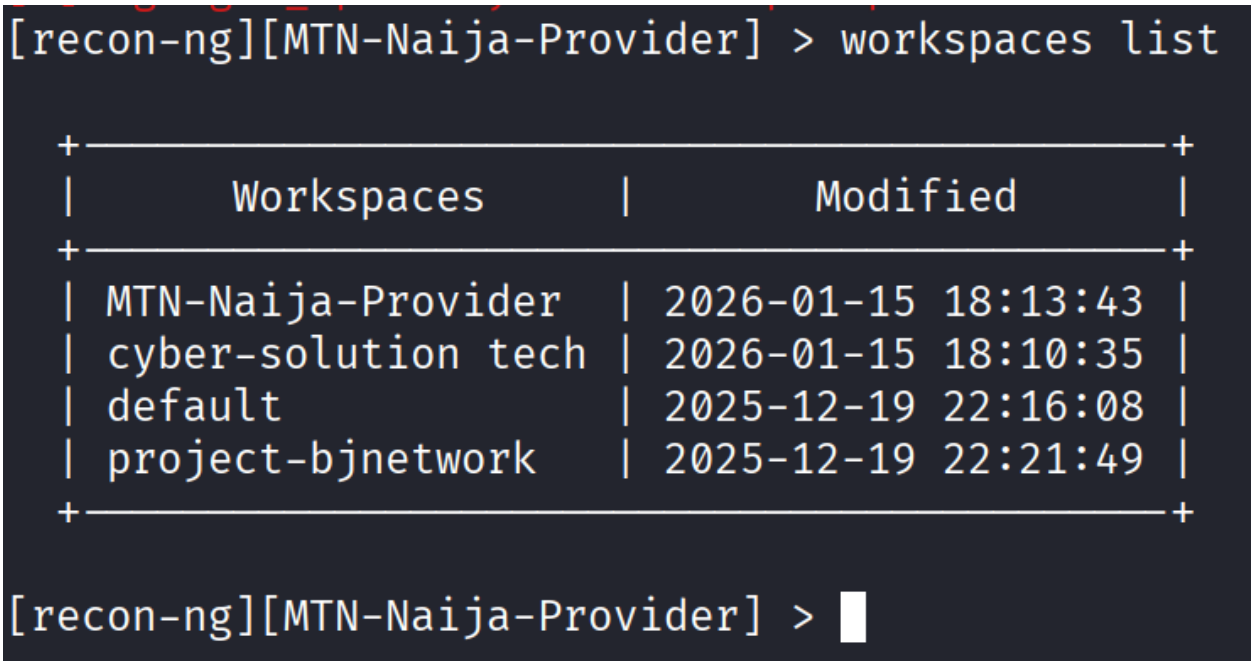
Step 1: Create Workspace

bash

recon-ng

workspaces create target_recon





Step 2: Add Target Domain

bash

db insert domains

 # Enter domain when prompted (e.g., example.com)

Phase 2: Module Installation

Step 3: Install Essential Modules

bash

marketplace install recon/domains-hosts/google_site_web

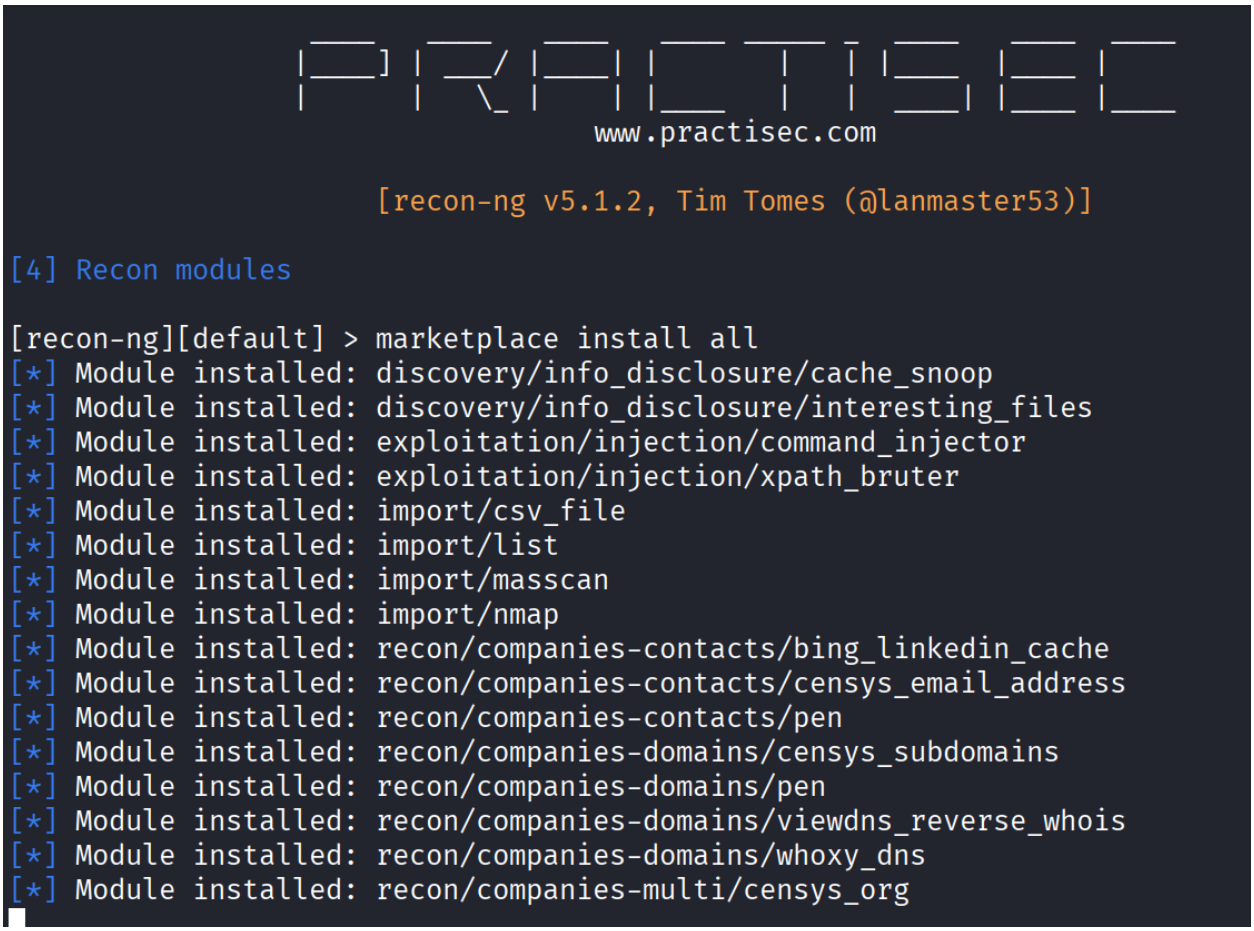
marketplace install recon/domains-hosts/bing_domain_web

marketplace install recon/hosts-hosts/resolve

marketplace install recon/domains-contacts/whois_pocs

marketplace install recon/netblocks-companies/whois_orgs

marketplace install discovery/info_disclosure/interesting_files



Phase 3: Information Gathering

Step 4: DNS Enumeration

bash

modules load recon/domains-hosts/google_site_web

options set SOURCE example.com

Run

```
[recon-ng][project-bjnetwork] > marketplace search

  +-------------------------------------------------------------------------------+
  |                          Path                          | Version |   Status  |  Updated   | D | K |
  +-------------------------------------------------------------------------------+
  | discovery/info_disclosure/cache_snoop                  | 1.1     | installed | 2020-10-13 |   |   |
  | discovery/info_disclosure/interesting_files            | 1.2     | installed | 2021-10-04 |   |   |
  | exploitation/injection/command_injector                | 1.0     | installed | 2019-06-24 |   |   |
  | exploitation/injection/xpath_bruter                    | 1.2     | installed | 2019-10-08 |   |   |
  | import/csv_file                                        | 1.1     | installed | 2019-08-09 |   |   |
  | import/list                                            | 1.1     | installed | 2019-06-24 |   |   |
  | import/masscan                                         | 1.0     | installed | 2020-04-07 |   |   |
  | import/nmap                                            | 1.1     | installed | 2020-10-06 |   |   |
  | recon/companies-contacts/bing_linkedin_cache           | 1.0     | installed | 2019-06-24 |   | * |
  | recon/companies-contacts/censys_email_address          | 2.1     | installed | 2022-01-31 | * | * |
  | recon/companies-contacts/pen                           | 1.1     | installed | 2019-10-15 |   |   |
  | recon/companies-domains/censys_subdomains              | 2.1     | disabled  | 2022-01-31 | * | * |
  | recon/companies-domains/pen                            | 1.1     | installed | 2019-10-15 |   |   |
  | recon/companies-domains/viewdns_reverse_whois          | 1.1     | installed | 2021-08-24 |   |   |
  | recon/companies-domains/whoxy_dns                      | 1.1     | installed | 2020-06-17 |   | * |
  | recon/companies-multi/censys_org                       | 2.1     | installed | 2022-01-31 | * | * |
  | recon/companies-multi/censys_tls_subjects              | 2.1     | installed | 2022-01-31 | * | * |
  | recon/companies-multi/github_miner                     | 1.1     | installed | 2020-05-15 |   | * |
  | recon/companies-multi/shodan_org                       | 1.1     | installed | 2020-07-01 | * | * |
  | recon/companies-multi/whois_miner                      | 1.1     | installed | 2019-10-15 |   |   |
```

```
bjnetwork@bjnetwork: ~
Session  Actions  Edit  View  Help
  | recon/ports-hosts/migrate_ports                      | 1.0     | installed | 2019-06-24 |   |   |
  | recon/ports-hosts/ssl_scan                           | 1.1     | installed | 2021-08-24 |   |   |
  | recon/profiles-contacts/bing_linkedin_contacts       | 1.2     | installed | 2021-08-24 |   | * |
  | recon/profiles-contacts/dev_diver                    | 1.1     | installed | 2020-05-15 |   |   |
  | recon/profiles-contacts/github_users                 | 1.0     | installed | 2019-06-24 |   | * |
  | recon/profiles-profiles/namechk                      | 1.0     | installed | 2019-06-24 |   | * |
  | recon/profiles-profiles/profiler                     | 1.2     | installed | 2023-12-30 |   |   |
  | recon/profiles-profiles/twitter_mentioned            | 1.0     | installed | 2019-06-24 |   | * |
  | recon/profiles-profiles/twitter_mentions             | 1.0     | installed | 2019-06-24 |   | * |
  | recon/profiles-repositories/github_repos             | 1.1     | installed | 2020-05-15 |   | * |
  | recon/repositories-profiles/github_commits           | 1.0     | installed | 2019-06-24 |   | * |
  | recon/repositories-vulnerabilities/gists_search      | 1.0     | installed | 2019-06-24 |   |   |
  | recon/repositories-vulnerabilities/github_dorks      | 1.0     | installed | 2019-06-24 |   | * |
  | reporting/csv                                        | 1.0     | installed | 2019-06-24 |   |   |
  | reporting/html                                       | 1.0     | installed | 2019-06-24 |   |   |
  | reporting/json                                       | 1.0     | installed | 2019-06-24 |   |   |
  | reporting/list                                       | 1.0     | installed | 2019-06-24 |   |   |
  | reporting/proxifier                                  | 1.0     | installed | 2019-06-24 |   |   |
  | reporting/pushpin                                    | 1.0     | installed | 2019-06-24 |   | * |
  | reporting/xlsx                                       | 1.0     | installed | 2019-06-24 |   |   |
  | reporting/xml                                        | 1.1     | installed | 2019-06-24 |   |   |
  +-------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][project-bjnetwork] >
```

Step 6: Subdomain Discovery

bash

modules load recon/domains-hosts/bing_domain_web

options set SOURCE example.com

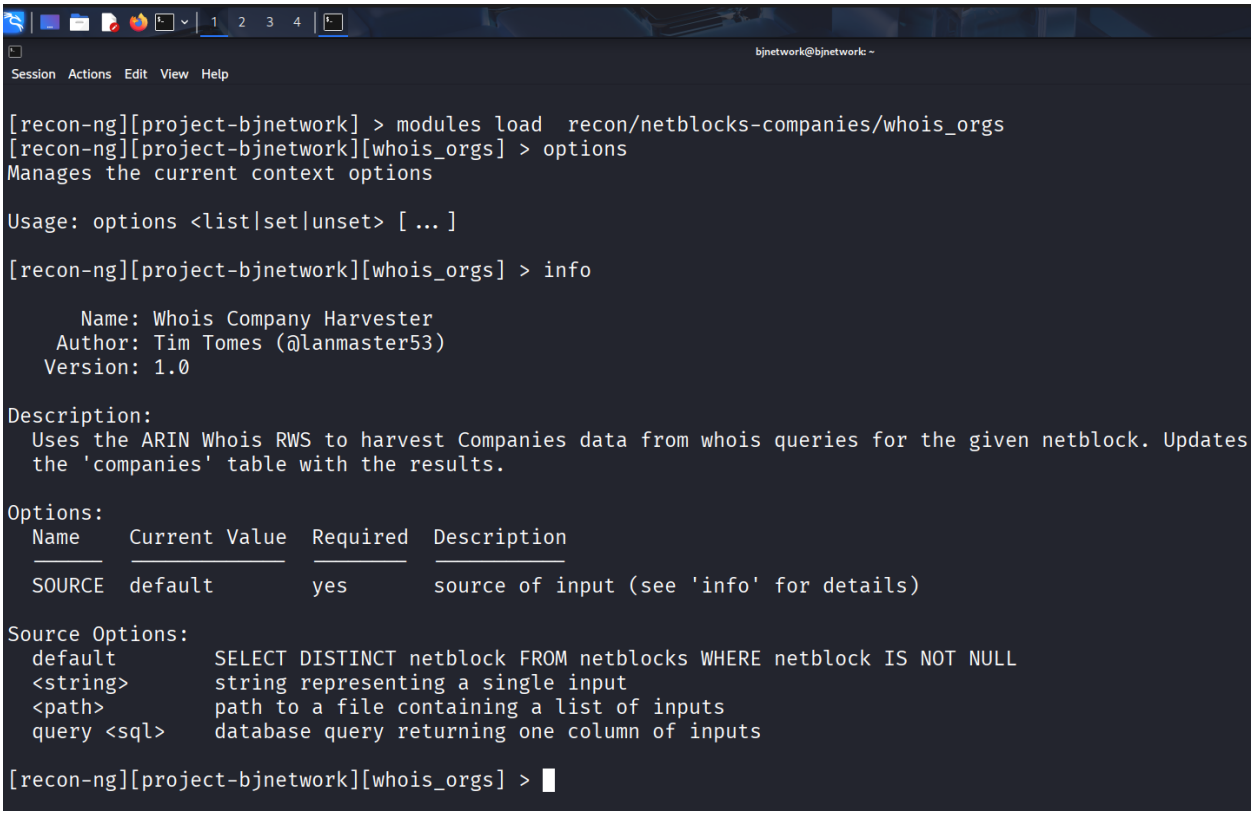
run

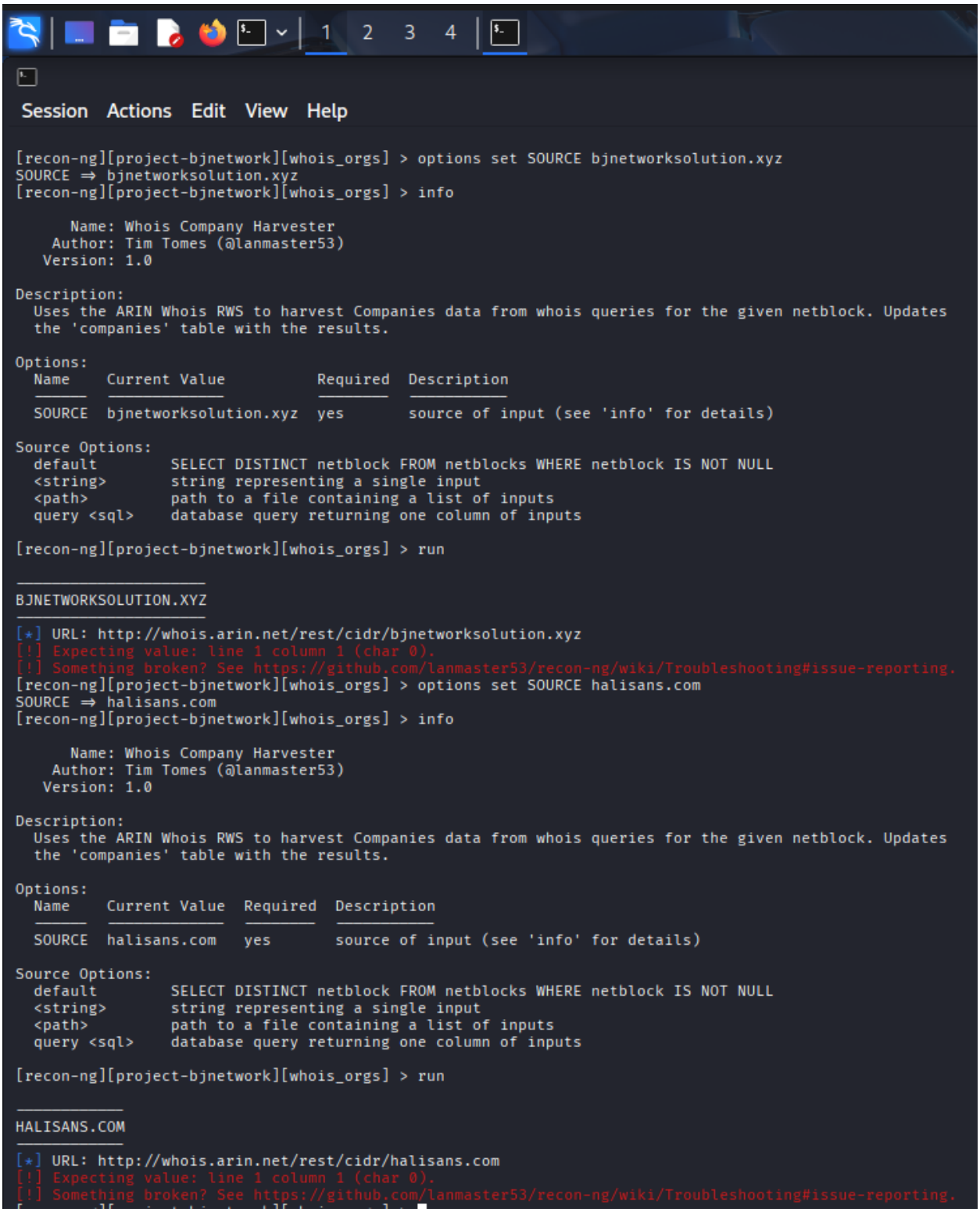
Step 7: Host Resolution

bash

modules load recon/hosts-hosts/resolve

Run




1 2 3 4
Session Actions Edit View Help
[recon-ng][project-bjnetwork][whois_orgs] > options set SOURCE bjnetworksolution.xyz
SOURCE => bjnetworksolution.xyz
[recon-ng][project-bjnetwork][whois_orgs] > info
Name: Whois Company Harvester
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Description:
Uses the ARIN Whois RWS to harvest Companies data from whois queries for the given netblock. Updates the 'companies' table with the results.
Options:
Name Current Value Required Description
SOURCE bjnetworksolution.xyz yes source of input (see 'info' for details)
Source Options:
default SELECT DISTINCT netblock FROM netblocks WHERE netblock IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][project-bjnetwork][whois_orgs] > run
BJNETWORKSOLUTION.XYZ
[*] URL: http://whois.arin.net/rest/cidr/bjnetworksolution.xyz
[!] Expecting value: line 1 column 1 (char 0).
[!] Something broken? See https://github.com/lanmaster53/recon-ng/wiki/Troubleshooting#issue-reporting.
[recon-ng][project-bjnetwork][whois_orgs] > options set SOURCE halisans.com
SOURCE => halisans.com
[recon-ng][project-bjnetwork][whois_orgs] > info
Name: Whois Company Harvester
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Description:
Uses the ARIN Whois RWS to harvest Companies data from whois queries for the given netblock. Updates the 'companies' table with the results.
Options:
Name Current Value Required Description
SOURCE halisans.com yes source of input (see 'info' for details)
Source Options:
default SELECT DISTINCT netblock FROM netblocks WHERE netblock IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][project-bjnetwork][whois_orgs] > run
HALISANS.COM
[*] URL: http://whois.arin.net/rest/cidr/halisans.com
[!] Expecting value: line 1 column 1 (char 0).
[!] Something broken? See https://github.com/lanmaster53/recon-ng/wiki/Troubleshooting#issue-reporting.

Phase 4: Data Review

Step 8: Examine Collected Data

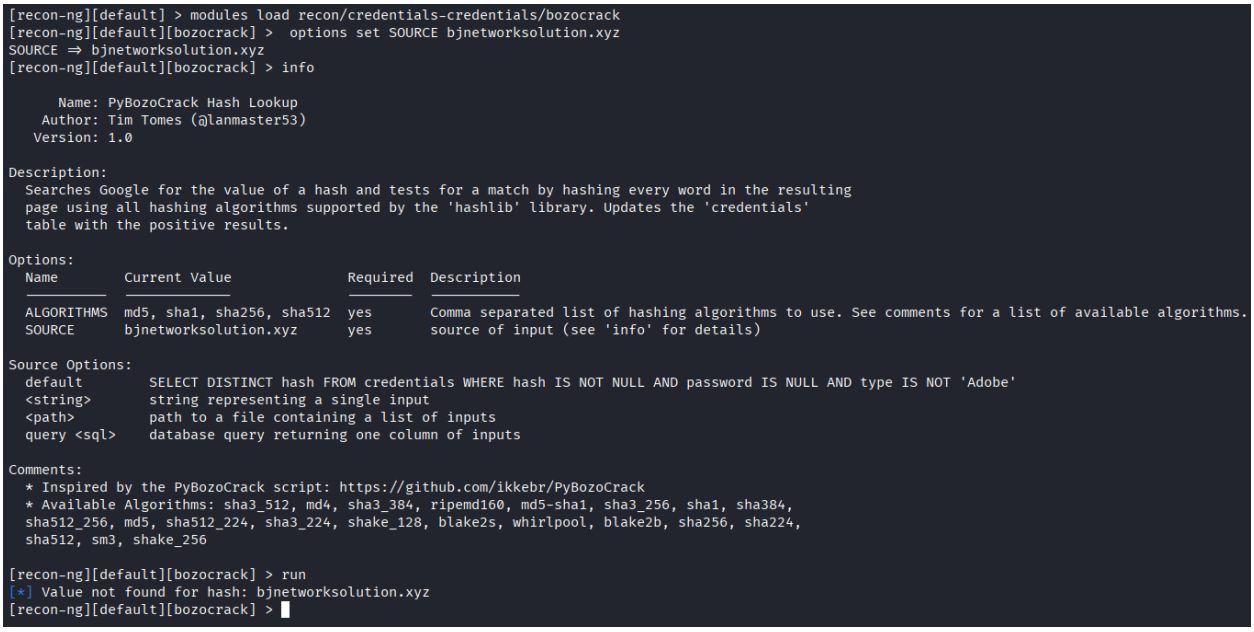
bash

show hosts

show contacts

show domains

show companies



```
[recon-ng][default] > modules load  recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] >  options set SOURCE bjnetworksolution.xyz
SOURCE => bjnetworksolution.xyz
[recon-ng][default][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value          Required  Description
  ------  ---------------        --------  -----------
  SOURCE  bjnetworksolution.xyz  yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][hackertarget] > run

-----------------------
BJNETWORKSOLUTION.XYZ
-----------------------
[*] Country: None
[*] Host: bjnetworksolution.xyz
[*] Ip_Address: 44.230.85.241
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------------

-------
SUMMARY
-------
[*] 1 total (1 new) hosts found.
[recon-ng][default][hackertarget] >
```

```
[recon-ng][default][hackertarget] > show
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default][hackertarget] > show hosts

  +-------------------------------------------------------------------------------------------------+
  | rowid |          host          |   ip_address   | region | country | latitude | longitude | notes |    module    |
  +-------------------------------------------------------------------------------------------------+
  | 1     | halisans.com           | 66.29.153.49   |        |         |          |           |       | hackertarget |
  | 2     | bjnetworksolution.xyz  | 44.230.85.241  |        |         |          |           |       | hackertarget |
  +-------------------------------------------------------------------------------------------------+

[*] 2 rows returned
[recon-ng][default][hackertarget] >
```

Information Analysis

Critical Information to Look For

During Scanning

1. **Subdomains**: Identify attack surface expansion
2. **Email Addresses**: Potential phishing targets or social engineering vectors
3. **Employee Names**: Social engineering reconnaissance
4. **IP Addresses**: Network infrastructure mapping
5. **Technologies Used**: Identify potential vulnerabilities
6. **DNS Records**: Understand network configuration
7. **Exposed Services**: Find potential entry points

After Scanning

1. **Pattern Recognition**: Look for naming conventions
2. **Infrastructure Analysis**: Cloud vs on-premise hosting
3. **Third-party Services**: Identify external dependencies
4. **Data Leaks**: Exposed credentials or sensitive information
5. **Attack Surface**: Entry points for penetration testing

How to Use This Information

For Security Professionals

- **Penetration Testing**: Identify targets for authorized testing
- **Vulnerability Assessment**: Discover exposed services
- **Security Auditing**: Evaluate organizational exposure
- **Incident Response**: Map infrastructure during investigations

For Red Team Operations

- **Social Engineering**: Build targeted phishing campaigns
- **Infrastructure Mapping**: Understand network topology
- **Vulnerability Exploitation**: Identify weak points
- **Persistence Planning**: Find stable infrastructure points

For Blue Team Defense

- **Asset Discovery**: Know what you're protecting
- **Exposure Reduction**: Remove unnecessary public information
- **Monitoring**: Set up alerts for exposed services
- **Security Posture**: Understand external visibility

Advantages & Disadvantages

Advantages

1. **Modular Architecture**
    - Use only needed modules
    - Easy to extend functionality
    - Community-driven development
2. **Database Integration**
    - Organized data storage
    - Relational data management
    - Easy data querying and export
3. **Automation**
    - Reduce manual OSINT work
    - Consistent methodology
    - Time-efficient reconnaissance
4. **Professional Output**
    - Multiple report formats
    - Structured data presentation
    - Easy to share findings
5. **Active Development**
    - Regular updates
    - Growing module marketplace

- Community support

Disadvantages

1. **API Key Dependency**
    - Many modules require API keys
    - Rate limiting on free APIs
    - Cost for premium services
2. **Learning Curve**
    - Command-line interface complexity
    - Module understanding required
    - Database knowledge helpful
3. **Legal Considerations**
    - Must have authorization
    - Potential for misuse
    - Ethical boundaries required
4. **Data Accuracy**
    - Depends on source reliability
    - May contain outdated information
    - False positives possible
5. **Detection Risk**
    - Activities may be logged
    - IP address exposure
    - Rate limiting triggers

Security Best Practices

Legal & Ethical Guidelines

1. **Authorization First**
    - Always obtain written permission
    - Stay within scope boundaries
    - Document all activities
2. **Responsible Disclosure**
    - Report findings to proper channels
    - Allow time for remediation
    - Don't publicly disclose vulnerabilities prematurely

Operational Security

3. **Use VPN/Proxy**

bash

```
# Configure proxy in Recon-ng
options set PROXY http://proxy-address:port
```

4. **API Key Protection**
    - Never share API keys
    - Use environment variables
    - Rotate keys regularly

bash

```
keys add shodan_api <your_key>
```

5. **Data Protection**
    - Encrypt sensitive findings
    - Secure workspace databases
    - Delete data when project completes

bash

```
# Backup workspace
```

```
cp ~/.recon-ng/workspaces/<name>/<name>.db /secure/location/
```

6. **Rate Limiting Awareness**
    - Respect API limits
    - Add delays between requests
    - Use multiple API keys if authorized
7. **Attribution Avoidance**
    - Don't use personal accounts
    - Vary reconnaissance patterns
    - Clear browser cookies/cache

Technical Safeguards

8. **VM Isolation**
    - Use snapshots before testing
    - Isolate reconnaissance VM
    - Don't mix with production systems
9. **Log Management**
    - Review Recon-ng logs
    - Clear sensitive command history

bash

```
history -c  # Clear bash history
```

10. **Regular Updates**

bash

```
marketplace refresh  # Update module marketplace
cd /opt/recon-ng && git pull  # Update Recon-ng
```

Quick Reference Card

Common Workflow

bash

 # 1. Start and setup

recon-ng

workspaces create project_name

 # 2. Add targets

db insert domains

 # 3. Install modules

marketplace install all

 # 4. Run reconnaissance

modules load <module>

options set SOURCE target.com

run

 # 5. Review results

show hosts

show contacts

 # 6. Generate report

modules load reporting/html

run

Useful Module Categories

- recon/domains-hosts/* - Subdomain enumeration
- recon/hosts-hosts/* - Host information gathering
- recon/domains-contacts/* - Email/contact discovery
- discovery/info_disclosure/* - Information leaks
- reporting/* - Report generation

Troubleshooting

Common Issues

Module won't install

bash

marketplace refresh

marketplace install <module> --force

API key errors

bash

keys list *# Verify keys are set*

keys add <service> <key>

No results returned

- Verify target domain is correct
- Check API key quotas
- Try alternative modules
- Review module options

Conclusion

Recon-ng and Recon-web are powerful reconnaissance tools that, when used ethically and legally, provide invaluable intelligence for security professionals. Always prioritize authorization, responsible disclosure, and operational security in your reconnaissance activities.

Remember: With great power comes great responsibility. Use these tools only for authorized security testing and research.